Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®

Journal of Symbolic Computation

Strongly Noetherian rings and constructive ideal theory

Hervé Perdry[*,1]

Departamento de Matematicas, Estadistica y Computación, Facultad de Ciencias, Universidad de Cantabria, Avenida de los Castros s/n, Santander 39071, Cantabria, Spain

Received 19 April 2002; accepted 6 February 2003

Abstract

We give a new constructive definition for Noetherian rings. It has a very concrete statement and is nevertheless strong enough to prove constructively the termination of algorithms involving "trees of ideals". The efficiency of such algorithms (at least for providing clear and intuitive constructive proofs) is illustrated in a section about Lasker–Noether rings: we give constructive proofs for the existence of the minimal primes over an ideal, of its radical, of its primary decomposition, in a wide class of polynomial rings.

Keywords: Noetherian ring

0. Introduction

In the year 1890, David Hilbert published the following result (cf. Hilbert, 1890, Theorem 1):

Theorem A. *Let F be a field. Let $f_1, f_2, \ldots$ be homogeneous polynomials in $F[x_1, \ldots, x_d]$. There exists $n \in \mathbb{N}$ such that for all $i \in \mathbb{N}$, the polynomial f_i can be written as*

$$f_i = a_1 \cdot f_1 + \cdots + a_n \cdot f_n$$

where $a_1, \ldots, a_n$ are homogeneous polynomials.

* Tel.: +34-942-201-440; fax: +34-942-201-402.
E-mail address: herve@matesco.unican.es (H. Perdry).

1 Most of this paper was written in the Équipe de Mathématiques de Besançon, UMR CNRS 6623, Université de Franche-Comté, Besançon, France.

0747-7171/$ - see front matter
doi:10.1016/j.jsc.2003.02.001

Note that the article quoted above, as well as Hermann's and Gordan's articles quoted below, can be downloaded on the *Göttinger Digitalisierungs-Zentrum*, web address http://www.gdz.sub.uni-goettingen.de/.

This highly non-constructive result was difficult to accept at the time. The reaction of Gordan (authentic or not) *"Das ist nicht Mathematik, das ist Theologie!"* is often quoted. Indeed, Hilbert used this result in the context of invariant theory to prove the existence of a finite basis of a system of invariants, without actually providing such a basis, which was both deceiving and shocking. Later, Hilbert gave a constructive proof for this last result.

Nowadays, "Hilbert's basis theorem" refers to the following equivalent statement:

Theorem B. *Let F be a field; every ideal of the ring $R = F[X_1, \ldots, X_d]$ admits a finite basis.*

In this paper, we adopt a constructive point of view in the sense of Bishop (1967), which is in our opinion the prolongation of previous works of Kronecker or Hermann (Hermann, 1926) (an English translation is available in Hermann, 1998).

From this point of view, this result does not hold: it is definitively impossible to give an algorithmic way to extract a finite basis from an explicitly given infinite enumeration of polynomials.

More precisely, for a given Turing machine T, define elements f_i of a (non-trivial) field F as follows: $f_0 = 0$, $f_i = 1$ if T stops at step i, else $f_i = 0$. One can compute as many of the f_i as wanted, so this enumeration is explicitly given. Now, to give a basis of the ideal of F generated by $f_0, f_1, \ldots$ means to solve the halting problem for T, which is impossible.

0.1. Noether's ascending chain condition

Let $(E, \leq)$ be a poset. The classical ascending chain condition, introduced by Emmy Noether in the early twentieth century, reads as follows:

ACC$_\circ$ If $(a_i)_{i\in\mathbb{N}}$ is a weakly increasing sequence, there exists some index $n \in \mathbb{N}$ such that $a_n = a_{n+1} = a_{n+2} = \cdots$.

Note that every ring in this paper is supposed to be commutative. A ring R is said to be *Noetherian* if the poset $(\mathcal{J}_R, \subseteq)$ of all ideals of R satisfies **ACC$_\circ$**. In classical mathematics, it is easy to verify that a ring R is Noetherian if and only if every ideal of R admits a finite basis.

Hilbert's basis theorem can then be restated as follows:

Theorem C. *Let F be a field; the ring $R = F[X_1, \ldots, X_d]$ is Noetherian.*

And "Hilbert's basis theorem" sometimes refers improperly to the following statement:

Theorem D. *If R is a Noetherian ring, then so is $R[X]$.*

Note that (in classical mathematics again) a field F is a Noetherian ring, so that Theorem D implies Theorem C.

If one restricts this definition to the poset $(\mathcal{I}_R, \subseteq)$ of *finitely generated* ideals, one obtains an equivalent (from the classical point of view) definition which seems to make more sense from the constructive point of view. Unfortunately, it appears that (again from this viewpoint) the sole trivial ring $R = 0$ is Noetherian: the same Turing machine argument holds again.

It is worth noting that the classical proof of Theorem D is constructive, the problem is that no non-trivial ring satisfies *constructively* the *classical* ascending chain condition.

0.2. Algorithmic consequences

The ascending chain condition in polynomial rings has lots of algorithmic consequences. The best known is undoubtedly the termination of Buchberger's algorithm, which computes the Gröbner basis of an ideal in a ring $F[X_1, \ldots, X_d]$ where F is a field. More details on this point shall be given in Section 1.

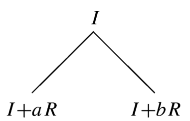
Let us turn to another kind of problem: the following theorem is well-known (cf. e.g. Malliavin, 1985).

Theorem E. *Let I be an ideal in a Noetherian ring R. There exists finitely many prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_q$ containing I, such that if $\mathfrak{P}$ is a prime ideal containing I, there exists i such that $I \subseteq \mathfrak{P}_i \subseteq \mathfrak{P}$.*

Proof (Classical). Let $\mathcal{F}$ be the family of all ideals not satisfying this property. R is Noetherian, so if $\mathcal{F}$ is non-empty we can choose a maximal element I in $\mathcal{F}$. I is in $\mathcal{F}$, so it is not prime; take $a, b \in R$ such that $ab \in I$ and $a, b \notin I$. The ideals $I + aR$ and $I + bR$ are strictly greater than I, hence not in $\mathcal{F}$; there exists finitely many primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ and $\mathfrak{P}_{r+1}, \ldots, \mathfrak{P}_q$ containing each, with the property stated in the lemma. Any prime ideal $\mathfrak{P}$ above I contains $I + aR$ or $I + bR$, so contains one of the $\mathfrak{P}_1, \ldots, \mathfrak{P}_q$; this is a contradiction, so $\mathcal{F}$ is empty. □

Let us suppose that there exists a way to decide whether a finitely generated ideal I of R is prime or not, and if not, to produce $a, b \in R$ such that $ab \in I$ and $a, b \notin I$. The previous proof can then be turned into an algorithmic version:

Proof (Computer Algebra). Let I be an ideal. If I is prime, let $\mathfrak{P}_1 = I$ and we are done. If not, let $a, b \in R$ such that $ab \in I$ and $a, b \notin I$. Begin to construct the following tree:



and apply the test to each leaf of the tree. In this way, we construct a binary tree, with nodes labeled by ideals of R, such that, along each branch of it, there is an increasing sequence of ideals. Then each branch is finite; so, by König's lemma, or more precisely, its contrapositive (equivalent in the context of classical mathematics), the tree is finite. The ideals labeling the leaves of this tree are the minimal primes containing I. □

For this algorithm as well as for Buchberger's algorithm, the situation is the following: the classical proofs of termination of these algorithm are not constructive.

Giving constructive proofs for this kind of result is a necessity from the point of view of constructive mathematics; it can as well be of some interest from the strict point of view of computer algebra. Constructive proofs can provide bounds to the number of steps after which the algorithm stops, as shown in Perdry (2001); unfortunately, in this case, the bounds are not primitive recursive, and are too large to be useful.

0.3. Constructive solutions

A good way to deal with this problem is to *change* the definition of Noetherian rings. The key criteria for a good new definition of Noetherian rings are the following:

- It must be, from the point of view of classical mathematics, equivalent to the classical definition.
- It must hold, from the constructive point of view, at least for fields and for most usual Noetherian rings.
- One must be able to prove constructively that if it holds for a ring R, it is inherited by $R[X]$.

Of course we hope that this new definition makes the natural proofs of termination of the greatest possible number of algorithms constructive.

Various such definitions have been given by several authors: we give here a short summary of some of these.

We need to give a few definitions (classical in constructive mathematics, cf. e.g. Mines et al., 1988).

Definition.
- A ring R (or a field F) is said to be *discrete* if the equality is decidable; that is, we have an effective way to decide whether a given a is zero or not.
- A ring R is *coherent* if for all $a_1, \dots, a_n \in R$, the kernel of the map

$$R^n \longrightarrow R$$
$$(x_1, \dots, x_n) \mapsto a_1 \cdot x_1 + \cdots + a_n \cdot x_n$$

  is finitely generated. This submodule of R^n is the *syzygy module* of the ideal $\langle a_1, \dots, a_n\rangle \in \mathcal{I}_R$.
- A ring R has *detachable ideals* if for all $b, a_1, \dots, a_n \in R$, the following holds constructively:

$$b \in \langle a_1, \dots, a_n\rangle \qquad \text{or} \qquad b \notin \langle a_1, \dots, a_n\rangle.$$

Remark. In constructive mathematics, a disjunction of the type $\forall x, A(x) \vee B(x)$ holds if, and only if, for any given x, one can decide that $A(x)$ is true, or decide that $B(x)$ is true.

Hence an alternative formulation of the definition of discrete rings could have been: the excluded middle ($a = 0$ or $a \neq 0$) holds constructively.

The definition of coherent rings means that given $a_1, \dots, a_n \in R$ you have an *effective* way to find generators $g_1, \dots, g_m$ of the syzygy module, and, given $x = (x_1, \dots, x_n)$ such that $\sum_i a_i \cdot x_i = 0$, to find $\lambda_1, \dots, \lambda_m \in R$ such that $x = \lambda_1 \cdot g_1 + \cdots + \lambda_m \cdot g_m$.

Classically, every Noetherian ring is coherent, but this is not provable constructively (that is, there is no general algorithm computing a base of the syzygy module of a given finitely generated ideal). We shall have to add this condition to the rings we deal with.

The definition of rings with detachable ideals is intended to look odd: the statement holds *constructively* in a ring R if we have an *effective* way, given $b, a_1, \dots, a_n \in R$, to decide whether b is in $\langle a_1, \dots, a_n\rangle$ or not, and in the first case, to produce $x_1, \dots, x_n$ such that $b = x_1 \cdot a_1 + \cdots + x_n \cdot a_n$.

Notation. In a ring R, we denote $(\mathcal{I}_R, \subseteq)$ the poset of finitely generated ideals.

0.3.1. The Richman–Seidenberg condition

In 1974, Richman and Seidenberg gave the following version of the ascending chain condition (cf. Richman, 1974; Seidenberg, 1974, and the book "A Course in Constructive Algebra" (Mines et al., 1988)):

ACC If $(a_i)_{i\in\mathbb{N}}$ is a weakly increasing sequence, there exists some index $n \in \mathbb{N}$ such that $a_n = a_{n+1}$.

From the classical viewpoint the two conditions $\mathbf{ACC}_\circ$ and **ACC** are equivalent (using excluded middle, both mean that increasing sequences in E are finite). But for constructivists, this condition is weaker, and can be satisfied by non-trivial posets.

Definition. Let R be a ring; the set of *finitely generated ideals* of R is denoted $\mathcal{I}_R$. The ring R is said to be RS-*Noetherian* if the poset $(\mathcal{I}_R, \subseteq)$ satisfies **ACC**.

In the above definition, the letters R and S stand for Richman and Seidenberg. Note that we have to restrict to finitely generated ideals; it is an easy exercise to prove that this definition is equivalent, in classical mathematics, to the classical one.

Now, from the constructive viewpoint, common rings like $\mathbb{Z}$ or $\mathbb{Q}$, or more generally discrete fields are RS-*Noetherian*. So it remains to prove a constructive version of Theorem D, to obtain a satisfying constructive theory of Noetherian rings.

The following theorem is Theorem VIII.1.5 from Mines et al. (1988):

Theorem F (Richman, Seidenberg). *If R is coherent and* RS-*Noetherian, so is $R[X]$. Moreover, if R has detachable ideals, so is $R[X]$.*

This condition is perfect to deal with the termination of algorithms such as Buchberger's algorithm (cf. Section 1).

Unfortunately, one cannot apply it to the proof of termination of Theorem E. Indeed, it proves that every branch of the binary tree stops; if one wanted to prove from this fact that the tree is finite, König's lemma (any infinite binary tree has an infinite path through it) should be invoked. More precisely, the following contrapositive form, known as the Fan theorem: if a binary tree has only finite branches, it is finite. This last theorem is accepted by intuitionists.

However, König's lemma and the Fan theorem are not constructive. In fact, there is even a recursive counter-example to both of them: Kleene constructed a recursive infinite binary tree whose every infinite branch is non-recursive (Beeson, 1985, p. 67). So it can be seen as an infinite tree where you will never be able to construct any infinite branch, so from a constructive point of view it has only finite branches.

This recursive tree can easily be used to produce a (recursive) poset in which **ACC** holds (for recursive sequences) but in which there is an infinite (recursive) binary tree with nodes labeled by elements such that along each branch of it there is an increasing sequence. A constructive proof, in our kroneckerian sense, would prevent the existence of such a recursive counter-example.

Remark. One of the anonymous referees of the paper made the following comment which is worth quoting here: "*This example of Kleene is a counter-example to the Fan Theorem, a fact that the intuitionists would interpret as showing that Church's thesis is false, so recursive counter-examples are worthless.*"

0.3.2. The Martin–Löf condition

Jacobsson and Löfwall (cf. Jacobsson and Löfwall, 1991) defined a nice notion of "blocked ideals", which allows to use "transfinite induction" to prove theorems about ideals of a Noetherian ring R.

Definition. Let $(E, \leq)$ be a poset. A subset H of E is *hereditary* if

$$\forall x, (\{y : y < x\} \subseteq H \Longrightarrow x \in H).$$

The poset E is *well-founded* if the only hereditary subset of E is $H = E$.

From a practical point of view this property allows to use induction in proofs.

Definition. A coherent ring with detachable ideals is ML-*Noetherian* if the poset $(\mathcal{I}_R, \supseteq)$ (with the reversed inclusion) is well-founded.

In the above definition, the letters M and L stand for Martin–Löf who suggested this definition. In classical mathematics, it is equivalent to the other definitions of Noetherian rings. In constructive mathematics, it is easy to prove that a ML-*Noetherian* ring is RS-*Noetherian*; the converse has no constructive proof. Jacobsson and Löfwall prove the following theorem:

Theorem G. *If R is a coherent* ML-*Noetherian ring with detachable ideals, so is $R[X]$.*

We reprove this result, cf. Theorem 2.1. If a ring is ML-*Noetherian*, in order to prove that a property c holds for all finitely generated ideals I, it suffices to prove that

$$(\forall J \supset I, c(J)) \Longrightarrow c(I).$$

We leave as an exercise to prove that in a ML-*Noetherian* ring, it is possible to prove constructively the termination of the algorithm sketched in the "computer algebra proof" of Theorem E.

This nice and powerful condition is sufficient to handle most of the concrete problems. Nevertheless, the following alternative definition is of interest.

0.3.3. Strongly Noetherian rings

We define here a new notion, *strongly Noetherian* rings.

Definition. A coherent ring R, with detachable ideals, is strongly Noetherian if there exists (explicitly) a decreasing map ϕ from $(\mathcal{I}_R, \subseteq)$ to a well-ordered set $(E, \leq)$.

A *well-ordered* set is a totally-ordered well-founded set.

Remark. We assume that equality as well as the order relation are decidable in $(E, \leq)$, which allows to consider without ambiguity the strict order relation in E. The ring R being assumed coherent with detachable ideals, the same is possible in $(\mathcal{I}_R, \subseteq)$; so there is no ambiguity on what is a *decreasing map* from $(\mathcal{I}_R, \subseteq)$ to $(E, \leq)$. We choose the classical definition

$$I \subset J \Longrightarrow \phi(I) > \phi(J)$$

and, using the fact that the order relations are decidable we obtain as an important consequence:

$$(I \subseteq J \wedge \phi(I) = \phi(J)) \Longrightarrow I = J.$$

That would not be the case without these hypotheses.

In many cases (that is, for rings which arise naturally in everyday algebra), one can assume that the well-ordered set in the above definition is $(\mathbb{N}^d, \leq_{\text{lex}})$ ($\leq_{\text{lex}}$ is the lexicographic order). We keep the general definition for the sake of generality.

Example H. The ring $\mathbb{Z}$ is strongly Noetherian: each finitely generated ideal is principal, so we map $\mathcal{I}_{\mathbb{Z}}$ to $\mathbb{N} \cup \{+\infty\}$, by $(0) \mapsto +\infty$ and for $a \neq 0$, $(a) \mapsto |a|$.

Example I. Let F be a discrete field. The ring $F[X]$ is strongly Noetherian; again, finitely generated ideals are principal, and we map $\mathcal{I}_{F[X]}$ to $\mathbb{N} \cup \{+\infty\}$, by $(0) \mapsto +\infty$ and for $f \neq 0$, $(f) \mapsto \deg f$.

Note that $\mathbb{N} \cup \{+\infty\}$ can be embedded in $(\mathbb{N}^2, \leq_{\text{lex}})$ by an increasing function, so we could use the restriction suggested above. In the case of multivariate polynomial rings over a field, the decreasing map will provide an analog of the degree. In the general case, the well-ordered set associated to a strongly Noetherian ring provides a kind of measure of complexity.

Moreover induction on $\phi(I)$ can be used in strongly Noetherian rings. In the case where $\phi(I)$ lives in $\mathbb{N}^d$ this is like doing d nested classical recursions in $\mathbb{N}$, so this is quite concrete. In particular, strongly Noetherian rings are ML-*Noetherian*: if H is a subset of $\mathcal{I}_R$ such that

$$(\forall J \supset I, J \in H) \Longrightarrow I \in H$$

we show that every $I \in \mathcal{I}_R$ is in H by induction on $\phi(I) \in E$ (remember that E is well-ordered). Assume that whenever $\phi(J) < \phi(I)$, we have $J \in H$; in particular, whenever $J \supset I$, J is in H, hence I is in H.

In fact strongly Noetherian rings are a special case of ML-*Noetherian* rings, which are themselves a special case of RS-*Noetherian* rings.

We are going to prove the following theorems:

Theorem J. *Let F be a discrete field. The ring $R = F[X_1, \ldots, X_d]$ is strongly Noetherian. Moreover, the map ϕ associated to R takes its values in* $(\mathbb{N}^d \cup \{+\infty\}, \leq_{\text{lex}})$.

Theorem K. *If R is a coherent, with detachable ideals and strongly Noetherian ring, so is $R[X]$.*

Theorem J will be proved (Theorem 1.3) using Gröbner bases and Buchberger's algorithm: we first prove strong Noetherianity for monomial ideals (so it is a new constructive proof of the so-called Dickson's lemma), deduce the correctness of Buchberger's algorithm, and we conclude by using the increasing map which associates to an ideal I the monomial ideal $\mathrm{LT}(I)$.

Theorem K will be built from building blocks provided by Mines et al. (1988), cf. Theorem 2.1. It can be used recursively to prove that $F[X_1, \dots, X_d]$ is strongly Noetherian in a much less efficient way. It would be nice to use Gröbner bases over rings (as developed in Jacobsson and Löfwall (1991) or Adams and Loustaunau (1994)) to give a better (less recursive) proof that $R[X_1, \dots, X_d]$ is strongly Noetherian, for an arbitrary strongly Noetherian ring R.

In Section 4, we return to the problem of finding the minimal primes over an ideal.

1. Polynomials over a field

In this section F is a discrete field; let d be a positive integer; R is the polynomial ring $F[X_1, \dots, X_d] = F[\underline{X}]$.

1.1. Gordan–Dickson lemma

If $\alpha \in \mathbb{N}^d$, we denote by $\underline{X}^\alpha$ the monomial $X_1^{\alpha_1} \cdots X_d^{\alpha_d}$.

Definition. An ideal of R generated by monomials is a *monomial ideal*. The set of finitely generated monomial ideals of R is denoted by $\mathcal{MI}_R$.

For $\alpha^1, \dots, \alpha^n \in \mathbb{N}^d$, we introduce the following notation:

$$\langle \alpha^1, \dots, \alpha^n \rangle = \{\gamma \in \mathbb{N}^d : \alpha^1 \leq_d \gamma \vee \cdots \vee \alpha^n \leq_d \gamma\}.$$

The subsets of $\mathbb{N}^d$ introduced by this notation are often called *staircases*.

The order $\leq_d$ is defined by $\beta \leq_d \gamma$ if, and only if, $\beta_1 \leq \gamma_1 \wedge \cdots \wedge \beta_d \leq \gamma_d$. There is a one-to-one order preserving correspondence between non-zero monomial ideals of R and the staircases of $\mathbb{N}^d$. The zero ideal (0) is in $\mathcal{MI}_R$, and verifies $(0) \subseteq I$ for all $I \in \mathcal{MI}_R$; it is naturally associated to a "bottom" staircase of $\mathbb{N}^d$: the empty set $\varnothing$.

The following lemma was often reproved in papers of the beginning of the twentieth century. The first published proof is, as far as we know, in Gordan (1899) (to prove Hilbert's theorem!). It is the keystone of Gröbner basis theory.

Lemma 1.1 (Gordan–Dickson Lemma, Classical). *The poset* $(\mathcal{MI}_R, \subseteq)$ *satisfies* $\mathbf{ACC}_\circ$.

Of course, stated in this form, this lemma cannot be proved constructively.

Lemma 1.2 (Gordan–Dickson Lemma, Constructive). *There exists a decreasing map from* $(\mathcal{MI}_R, \subseteq)$ *to* $(\mathbb{N}^d \cup \{+\infty\}, \leq_{\mathrm{lex}})$.

Definition. A *subspace of dimension* $d-k$ *of* $\mathbb{N}^d$ is a subset $H^{\overline{r}}_{\overline{\imath},d-k}$ of the form

$$H^{\overline{r}}_{\overline{\imath},d-k} = \{(x_1, \dots, x_d) : x_{i_1} = r_1 \wedge \cdots \wedge x_{i_k} = r_k\}$$

where $\overline{r} = (r_1, \dots, r_k) \in \mathbb{N}^k$, $\overline{\imath} = (i_1, \dots, i_k)$ and $1 \leq i_1 < \cdots < i_k \leq d$.

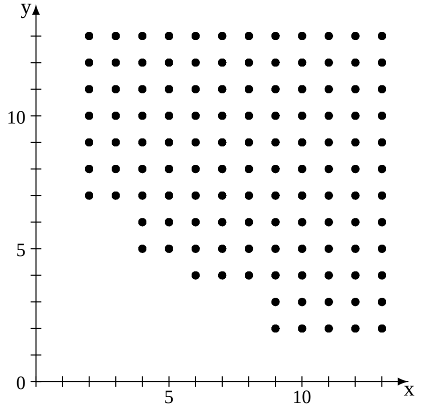


Fig. 1. A staircase for $d = 2$.

Note that subspaces of dimension 0 are singletons.

Proof. Take $\alpha^1, \ldots, \alpha^n \in \mathbb{N}^d$. We use the one-to-one correspondence defined above and look at $A = \langle \alpha^1, \ldots, \alpha^n \rangle \subseteq \mathbb{N}^d$ rather than at the associated monomial ideal.

Put $C_1 = \mathbb{N}^d \backslash A$. Let ψ_1 be the number of subspaces of dimension $d-1$ (not necessarily disjoint) included in C_1 (ψ_1 may be zero).

Let C_2 be C_1 minus these ψ_1 subspaces; there are ψ_2 subspaces of dimension $d - 2$ included in C_2. We carry on with this process until C_d which is a finite union of ψ_d singletons.

Denote $\Psi_d^\circ(\alpha_1, \ldots, \alpha_n) = (\psi_1, \ldots, \psi_d) \in \mathbb{N}^d$.

$$
\begin{aligned}
&\Psi_d : \mathcal{MI}_R \longrightarrow (\mathbb{N}^d \cup \{+\infty\}, \leq_{\text{lex}}) \\
&(0) \mapsto +\infty \\
&\underline{X}^{\alpha^1} \cdot R + \cdots + \underline{X}^{\alpha^n} \cdot R \mapsto \Psi_d^\circ(\alpha^1, \ldots, \alpha^n)
\end{aligned}
$$

is a decreasing map from $(\mathcal{MI}_R, \subseteq)$ to $(\mathbb{N}^d \cup +\{\infty\}, \leq_{\text{lex}})$. Indeed, if $A \subset A'$, then A' has a non-empty intersection with one of the $C_1, \ldots, C_d$. Let i be the smaller index such that $A' \cap C_i \neq \varnothing$, and let $\Psi_d(A') = (\psi'_1, \ldots, \psi'_d)$. Then $\psi_1 = \psi'_1, \ldots, \psi_{i-1} = \psi'_{i-1}$, and $\psi_i > \psi'_i$.

The above definition of Ψ_d relies on a geometric intuition. It is then of some interest to give some drawings for $d = 2$, $d = 3$.

Fig. 1 represents $A = \langle (2, 7), (4, 5), (6, 4), (9, 2) \rangle$.

The black dots are of course elements of A. We read easily $\Psi_2(A) = (4, 22)$: to be completed to $\mathbb{N}^2$, A needs 4 “lines” and 22 points.

It is clear that if $B \supsetneq A$ then either B cuts at least one of these 4 lines or B contains at least one of these 22 points; if $\psi_2(B) = (\psi_1, \psi_2)$, this means that either $\psi_1 < 4$ or $\psi_2 < 22$, i.e. $\Psi_2(B) <_{\text{lex}} \Psi_2(A)$.

Now turn to the case $d = 3$. Fig. 2 represents a staircase A of $\mathbb{N}^3$. The axes are not drawn for reason of readability; the origin is near to the reader, the directions of the axes

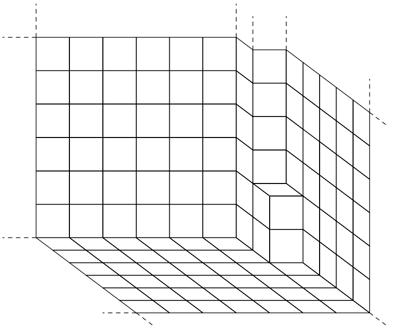


Fig. 2. A staircase for $d = 3$.

are indicated by the dotted lines. The point nearest to the reader is $(1, 1, 1)$, the two other points are $(3, 0, 1)$ and $(2, 0, 3)$. The reader will verify easily that $\Psi_d(A) = (2, 1, 2)$ (2 "planes", 1 "line" (vertical on our drawing), and 2 points are needed).

The given definition of Ψ_d° is, we think, concrete enough to deserve the qualification of "constructive". Nevertheless, it is better to give an effective computation algorithm for Ψ_d°. It is then convenient to define it recursively.

Let A be a staircase of $\mathbb{N}$; A can be written $A = \langle a \rangle$ with $a \in \mathbb{N}$, and $\Psi_1(A) = a$.

Let $\pi_1, \ldots, \pi_d$ be the d canonical projections of $\mathbb{N}^d$ onto $\mathbb{N}^{d-1}$. It is easy to compute effectively $\pi_i(A)$: if $A = \langle a_1, \ldots, a_n \rangle$, then $\pi_i(A) = \langle \pi_i(a_1), \ldots, \pi_i(a_n) \rangle$. Put

$$(\phi_1, \ldots, \phi_{d-1}) = \Psi_{d-1} \circ \pi_1(A) + \cdots + \Psi_{d-1} \circ \pi_d(A).$$

We can set $\psi_1 = \phi_1/(d-1), \ldots, \psi_{d-2} = \phi_{d-2}/2, \psi_{d-1} = \phi_{d-1}$.

It is a bit more difficult to compute ψ_d. We just sketch an algorithm. Assume again $A = \langle a_1, \ldots, a_n \rangle$. Let us call a *pad* of $\mathbb{N}^d$ a subset $\mathfrak{P}(a, b)$ defined for $a, b, \in \mathbb{N}_d$ with $a <_d b$ by:

$$\mathfrak{P}(a, b) = \{x \in \mathbb{N}^d : a \leq_d x <_d b\},$$

where $x <_d b$ means $x \leq_d b$ and $x \neq b$.

Close the family $a_1, \ldots, a_n$ by the operations $\vee_d$ and $\wedge_d$ defined by:

$$(\alpha_1, \ldots, \alpha_d) \vee_d (\beta_1, \ldots, \beta_d) = (\sup(\alpha_1, \beta_1), \ldots, \sup(\alpha_d, \beta_d))$$
$$(\alpha_1, \ldots, \alpha_d) \wedge_d (\beta_1, \ldots, \beta_d) = (\inf(\alpha_1, \beta_1), \ldots, \inf(\alpha_d, \beta_d)).$$

We obtain a finite set $\mathcal{A}$ of elements of $\mathbb{N}^d$, the boolean combinations of $a_1, \ldots, a_n$. In other words it is the lattice generated by $a_1, \ldots, a_n$.

Consider the pads $\mathfrak{P}_1, \ldots, \mathfrak{P}_\ell$ defined by pairs $a <_d b$ of elements of $\mathcal{A}$. This family is closed under intersection. Extract from it the family $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ of minimal pads for inclusion; these pads are disjoint. Each of these $\mathfrak{P}_i$ $(i \leq k)$ is either included in C_d or in the complement of C_d; if a pad $\mathfrak{P}$ is not included in A, but for all i, $\pi_i(\mathfrak{P}) \subseteq \pi_i(A)$, then $\mathfrak{P} \subseteq C_d$. On the other hand C_d is the disjoint union of those $\mathfrak{P}_i$ which intersect it, which allows to compute its cardinality ψ_d. $\square$

We obtain easily the following corollary. The **ACC** condition is the relevant one for the termination of division algorithm and Buchberger's algorithm.

Corollary 1.1. *The other constructive formulations of being Noetherian are consequences:*

- *The poset* $(\mathcal{MI}_R, \subseteq)$ *is well-founded.*
- *The poset* $(\mathcal{MI}_R, \subseteq)$ *satisfies* ***ACC***.

1.2. Some material: Gröbner bases

We recall here some background about Gröbner bases, one of the main tools of computer algebra. In Lombardi and Perdry (1998), we developed the idea that it is a natural and efficient tool for constructive algebra as well. For more details, in the proofs, see e.g. Cox et al. (1992). Gröbner bases were created in 1965 by Buchberger (cf. Buchberger, 1965, 1970). The proofs are constructive; the only difference with the classical proofs is that we use the constructive form of Dickson's lemma.

1.2.1. Monomial orderings, division

Definition. A total ordering $\preceq$ of $\mathbb{N}^d$ is *admissible* if:

- For all $\alpha \in \mathbb{N}^d$, $0 \preceq \alpha$.
- If $\alpha \preceq \beta$, then $\alpha + \gamma \preceq \beta + \gamma$.
- $\preceq$ is decidable.

We often note $\underline{X}^\alpha \preceq \underline{X}^\beta$ for $\alpha \preceq \beta$.

Example 1.1. The lexicographic order $\leq_{\text{lex}}$ is admissible.

Lemma 1.3. *If* $\preceq$ *is an admissible order of* $\mathbb{N}^d$*, then* $(\mathbb{N}^d, \preceq)$ *satisfies* ***ACC***.

Proof. Easy consequence of Corollary 1.1. □

Fix an admissible order $\preceq$ of $\mathbb{N}^d$. Let $f = \sum_{\alpha \in \mathbb{N}^d} a_\alpha \underline{X}^\alpha \in R$ be a non-zero polynomial. The multi-degree of f is

$$\operatorname{mdeg} f = \max_{\preceq}\{\alpha \in \mathbb{N}^d : a_\alpha \neq 0\}.$$

If $\alpha = \operatorname{mdeg} f$, the leading monomial, leading coefficient, and leading term of f are $\mathrm{LM}(f) = \underline{X}^\alpha$, $\mathrm{LC}(f) = a_\alpha$, and $\mathrm{LT}(f) = a_\alpha \underline{X}^\alpha$.

Proposition 1.1. *Take* $f_1, \ldots, f_s$ *in* $R = F[\underline{X}]$*. Every* $f \in R$ *can be effectively re-written as*

$$f = a_1 \cdot f_1 + \cdots + a_s \cdot f_s + r$$

where $a_1, \ldots, a_s, r \in R$, $\operatorname{mdeg} a_i \cdot f_i \preceq \operatorname{mdeg} f$*, and no monomial of* r *can be divided by one of the* $\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_s)$.
The polynomial r *is the* ***remainder of the division of*** f ***by*** $\mathcal{F} = (f_1, \ldots, f_s)$*. We denote it by* $r = \overline{f}^{\mathcal{F}}$.

Proof. If the following algorithm stops, the result is clearly what is expected.

Input: $f_1, \ldots, f_s, f$.
Output: $a_1, \ldots, a_s, r$.

$a_1 := 0, \ldots, a_s := 0,\ r := 0,\ p := f$
While $p \neq 0$ **do**
  $i := 1$**;**
  $div :=$ **false;**
  While ($i \leq s$ **and** $div =$ **false**) **do**
    If $\mathrm{LM}(f_i) \mid \mathrm{LM}(p)$ **then** $a_i := a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$**;**
      $p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$**;**
      $div :=$ **true.**
    else $i := i + 1$**.**
  If $div =$ **false, then** $r := r + \mathrm{LT}(p)$**,** $p := p - \mathrm{LT}(p)$**.**

The sequence of values of $\mathrm{LM}(p)$ is weakly decreasing for the monomial ordering, so it has to take the same value twice; this happens only for $p = 0$, hence the algorithm stops. □

Remark. The remainder is **not** unique.

1.2.2. Buchberger's algorithm

Definition. For all $\alpha, \beta \in \mathbb{N}^d$, we put $\sup_{\leq_d}(\alpha, \beta) = \gamma = (\gamma_1, \ldots, \gamma_d) \in \mathbb{N}^d$ where for all i, $\gamma_i = \max(\alpha_i, \beta_i)$. For all $f, g \in F[\underline{X}]$, if $\alpha = \operatorname{mdeg} f$, $\beta = \operatorname{mdeg} g$, and $\gamma = \sup_{\leq_d}(\alpha, \beta)$, the *S-polynomial of* f, g is

$$S(f, g) = \frac{\underline{X}^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{\underline{X}^\gamma}{\mathrm{LT}(g)} \cdot g.$$

We admit the following proposition (cf. Cox et al., 1992).

Proposition 1.2 (Buchberger). *Let $\mathcal{G} = (g_1, \ldots, g_s)$ be a family of elements of $R = F[\underline{X}]$. Put $I = g_1 \cdot R + \cdots + g_s \cdot R$. The following properties are equivalent:*

- *For all $f \in I$, the remainder $\overline{f}^{\mathcal{G}}$ is zero.*
- *For all $f \in I$, $\mathrm{LM}(f) \in \mathrm{LM}(g_1) \cdot R + \cdots + \mathrm{LM}(g_s) \cdot R$.*
- *For all i, j, $\overline{S(g_i, g_j)}^{\mathcal{G}} = 0$.*

*If these conditions hold, $\mathcal{G}$ is a **Gröbner basis** of I.*

We now state Buchberger's algorithm.

Theorem 1.2 (Buchberger's Algorithm). *Let $I = (f_1, \ldots, f_s)$ be a non-zero finitely generated ideal of R. The following algorithm computes a Gröbner basis of I:*

Input: $(f_1, \ldots, f_s)$ *a basis of* I.
Output: $\mathcal{G}$, *a Gröbner basis of* I.

$\mathcal{G} := (f_1, \ldots, f_s)$
Repeat
$H = \mathcal{G}$
For all $p, q \in H$ **do**
If $\overline{S(p,q)}^H \neq 0$ **then** $\mathcal{G} := \mathcal{G} \cup \left\{\overline{S(p,q)}^H\right\}$.
Until $H = \mathcal{G}$.

Proof. The previous proposition implies that if the algorithm stops, $\mathcal{G}$ is a Gröbner basis of I. At each step, consider the monomial ideal $\mathrm{LM}(\mathcal{G})$, generated by the leading monomials of the polynomials in $\mathcal{G}$: it is an increasing sequence in $\mathcal{MI}_R$, so the Richman–Seidenberg ascending condition (as well as our strong condition) suffices to ensure that it is finite, and the algorithm stops. □

1.3. $F[X_1, \ldots, X_d]$ is strongly Noetherian

This is now easy to conclude. The existence of Gröbner bases, now constructively proved allows to define the increasing map $\mathrm{LT} : \mathcal{I}_R \longrightarrow \mathcal{MI}_R$ which maps a finitely generated ideal I to the monomial ideal generated by the $\mathrm{LT}(f)$ for $f \in I$; Proposition 1.2 shows that it is a finitely generated ideal, generated by the leading terms of the polynomials in the Gröbner basis of I.

So the map

$$\begin{aligned} \mathcal{I}_R &\longrightarrow \mathcal{MI}_R \\ I &\mapsto \mathrm{LM}(I) \end{aligned}$$

is well-defined; it is an increasing map for the inclusion. We compose it with the map Ψ_d from Lemma 1.2 to obtain a decreasing map from $(\mathcal{I}_R, \subseteq)$ to $(\mathbb{N}^d, \leq_{\mathrm{lex}})$.

We have proved the following theorem:

Theorem 1.3. *Let F be a discrete field. The ring $R = F[X_1, \ldots, X_d]$ is strongly Noetherian. More precisely, there is a decreasing map from the set $\mathcal{I}_R$ of finitely generated ideals of R, ordered by the inclusion, to $\mathbb{N}^d \cup \{+\infty\}$ ordered lexicographically ($+\infty$ is a top element).*

Again, we have the following corollary:

Corollary 1.2. *Let F be a discrete field. The ring $R = F[X_1, \ldots, X_d]$ is* RS*-Noetherian and* ML*-Noetherian.*

2. Polynomials over a ring

In this section, R is a discrete, coherent ring with detachable ideals. Moreover R is assumed to be strongly Noetherian, hence RS-*Noetherian* and ML-*Noetherian*.

2.1. Some material: building blocks from Richman and Seidenberg

We give here, without proofs, some results from Mines et al. (1988). Proposition 2.1 comes from III.2.5 and III.2.7, Proposition 2.2 from VIII.1.2 and VIII.1.5, and Lemma 2.1 is Lemma VIII.1.4.

The definition of a coherent module is the natural generalization of the definition of a coherent ring (cf. the Introduction):

Definition. A R-module M is *coherent* if every finitely generated submodule N of M is *finitely presented*, that is, if $a_1, \dots, a_n$ are the generators of N, the kernel of the map

$$\begin{aligned} &R^n \longrightarrow N \\ &(x_1, \dots, x_n) \mapsto a_1 \cdot x_1 + \cdots + a_n \cdot x_n \end{aligned}$$

is finitely generated.

Of course we are speaking in the constructive sense, and in a coherent module, we have an effective way to find the generators of the kernel of the above map.

Proposition 2.1. *Let M be an R-module and N be a finitely generated R-submodule of M. Then M is coherent (and has detachable submodules) if, and only if, N and M/N are coherent (and have detachable submodules).*

Corollary 2.1. *If R is a coherent ring, then every finitely generated R-module of finite presentation (that is, the quotient of a free module of finite rank R^n by one of its finitely generated submodules) is coherent.*

For $n \in \mathbb{N}$, we denote by $R[X]_n$ the set of polynomials if degree $<n$. It is a free R-module of rank n.

Proposition 2.2. *Let R be a coherent (and with detachable ideals)* RS*-Noetherian ring.*

- *Take $I \in \mathcal{I}_{R[X]}$. Then $I \cap R[X]_n$ is a finitely generated R-module.*
- *The ring $R[X]$ is coherent (and has detachable ideals).*

If R is coherent and RS-*Noetherian*, take $I \in \mathcal{I}_{R[X]}$. We set

$$\text{LC}(I) = \{a \in R : \exists n, a_0, \dots, a_{n-1}, a \cdot X^n + a_{n-1} \cdot X^{n-1} + \cdots + a_0 \in I\}.$$

Lemma 2.1. *If R is coherent and* RS*-Noetherian, then for all $I \in \mathcal{I}_{R[X]}$, $\text{LC}(I)$ is finitely generated. If $I \subseteq J$ and $\text{LC}(I) = \text{LC}(J)$, then*

$$I \cap R[X]_n \textit{ generates } I \textit{ as an ideal} \Longrightarrow J \cap R[X]_n \textit{ generates } J.$$

2.2. Strongly Noetherian R-modules

If M is a finitely generated R-module, we denote by $\mathcal{I}_M$ the poset of finitely generated R-submodules of M. We shall say that M is strongly Noetherian if, and only if, there is a decreasing map from $\mathcal{I}_M$ to a well-ordered set $\mathcal{E}$, and that it is ML-*Noetherian* if, and only if, the poset $(\mathcal{I}_R, \subseteq)$ is well-founded.

Definition. Let $(E, \leq_E)$ and $(F, \leq_F)$ be two posets. The *product order* on $E \times F$ is defined by

$$(a, b) \leq_{E\times F} (a', b') \Longleftrightarrow (a \leq_E a') \wedge (b \leq_F b').$$

Lemma 2.2. *Let M be a coherent R-module and N a R-submodule of M. There is an increasing map from $\mathcal{I}_M$ to $\mathcal{I}_{M/N} \times \mathcal{I}_N$ (ordered by the product order).*

Proof. Put

$$\begin{aligned} &\psi : \mathcal{I}_M \longrightarrow \mathcal{I}_{M/N} \times \mathcal{I}_N \\ &A \mapsto (A/N, A \cap N). \end{aligned}$$

This map is well-defined, M being coherent. Order $\mathcal{I}_{M/N} \times \mathcal{I}_N$ by the product order; then Ψ is an increasing map: on the one hand if $A \subseteq B$ then $A/N \subseteq B/N$ and $A\cap N \subseteq B\cap N$. On the other hand if $A \subseteq B$, $A/N = B/N$ and $A \cap N = B \cap N$ then let b be an element of B; there exists some $a \in A$ such that $a + N = b + N$, hence $b - a \in B \cap N = A \cap N$; so $b - a \in A$ and $b \in A$; we have proved $A = B$. □

We admit the following two lemmas.

Lemma 2.3. *Let E and F be posets. If there is an increasing map from E to F, and F is well-founded, then E is well-founded.*

Lemma 2.4. *Let $(E_1, \leq_1)$ and $(E_2, \leq_2)$ be two posets. We denote by $E_1 \times E_2$ the direct product ordered by the product order, and by $E_1 \cdot E_2$ the direct product ordered by the lexicographic order.*

- *If E_1, E_2 are well-founded, then $E_1 \times E_2$ is well-founded.*
- *If E_1, E_2 are well-ordered, then $E_1 \cdot E_2$ is well-ordered.*

Proposition 2.3. *Let R be a coherent ring. Let M be a R-module and N a R-submodule of M.*

- *M is* ML*-Noetherian iff N and M/N are* ML*-Noetherian.*
- *M is strongly Noetherian iff N and M/N are strongly Noetherian.*

Proof. First point: the case of ML-*Noetherian* modules.

It is easy to find an increasing map from $\mathcal{I}_N$ to $\mathcal{I}_M$, and from $\mathcal{I}_{M/N}$ to $\mathcal{I}_M$. So if $\mathcal{I}_M$ is well-founded, Lemma 2.3 implies that $\mathcal{I}_N$ and $\mathcal{I}_{M/N}$ are well-founded.

If $\mathcal{I}_N$ et $\mathcal{I}_{M/N}$ are well-founded, so is $\mathcal{I}_{M/N} \times \mathcal{I}_N$, and we use the increasing map from $\mathcal{I}_M$ to $\mathcal{I}_{M/N} \times \mathcal{I}_N$ to conclude as before.

Second point: the case of strongly Noetherian modules.

Let $\phi_1 : \mathcal{I}_{M/N} \longrightarrow \mathcal{E}_1$ and $\phi_2 : \mathcal{I}_N \longrightarrow \mathcal{E}_2$ be decreasing maps to well-ordered posets $(\mathcal{E}_1, \leq_1)$ and $(\mathcal{E}_2, \leq_2)$.

The map

$$\begin{aligned} &\Psi : \mathcal{I}_M \longrightarrow \mathcal{E}_1 \cdot \mathcal{E}_2 \\ &A \mapsto (\phi_1(A/N), \phi_2(A \cap N)). \end{aligned}$$

is a decreasing map from $(\mathcal{I}_M, \subseteq)$ to $\mathcal{E}_1 \cdot \mathcal{E}_2 = (\mathcal{E}_1 \times \mathcal{E}_2, \leq_{\text{lex}})$ *ordered by the lexicographic order*, that is, a well-ordered set.

We leave the other implication to the reader. □

By induction, we obtain the following:

Corollary 2.2. *Let R be a coherent (with detachable ideals) ring. Let $n \in \mathbb{N}$; the free R-module R^n is coherent (and has detachable submodules). Moreover:*

- *If R is* ML*-Noetherian, so is R^n.*
- *If R is strongly Noetherian, so is R^n.*

2.3. $R[X]$ is strongly Noetherian

In this section R is coherent, has detachable ideals, and is at least RS-*Noetherian*.

Definition. For all $I \in \mathcal{I}_{R[X]}$ we define $n(I)$ as the smallest integer such that $I \cap R[X]_{n(I)}$ generates I as an ideal.

Note that if $I = (f_1, \ldots, f_s)$, $n(I)$ is lower or equal to the maximum of the degrees $\deg f_i$. It is possible to verify if $n \geq n(I)$ by first computing a basis $g_1, \ldots, g_t$ for the module $I \cap R[X]_n$ (Proposition 2.2) and testing whether $f_1, \ldots, f_s$ are in the ideal generated by the g_i's; so $n(I)$ is well-defined. Here we need R to have detachable ideals.

We can restate a part of the Lemma 2.1 as follows:

Lemma 2.5. *For $I, J \in \mathcal{I}_{R[X]}$, if $I \subseteq J$ and $\mathrm{LC}(I) = \mathrm{LC}(J)$ then $n(I) \geq n(J)$.*

Definition. Let $(\mathcal{E}_i, \leq_i)_{i\in\mathbb{N}}$ be a family of posets. We denote by $\overrightarrow{\bigoplus_{i\in\mathbb{N}}} \mathcal{E}_i \left(\text{resp. } \overleftarrow{\bigoplus_{i\in\mathbb{N}}} \mathcal{E}_i\right)$ the disjoint union of the $\mathcal{E}_i$'s ordered by:

$$x \in \mathcal{E}_i \preceq y \in \mathcal{E}_j \iff \begin{cases} i < j \,(\text{resp. } j < i). \\ \text{or } i = j \wedge x \leq_i y. \end{cases}$$

Note that if $(E'_i, \leq'_i) = (E_i, \geq_i)$, $\left(\overrightarrow{\bigoplus} \mathcal{E}'_i, \preceq\right) = \left(\overleftarrow{\bigoplus} \mathcal{E}_i, \succeq\right)$. That is the reason why we make two definitions: $\overrightarrow{\bigoplus}$ is all right when the $(E_i, \leq_i)$ are well-founded, $\overleftarrow{\bigoplus}$ shall be used when the reverse ordered sets $(E_i, \geq_i)$ are well-founded.

Lemma 2.6. *If the posets $(\mathcal{E}_i, \leq_i)_{i\in\mathbb{N}}$ are well-founded (resp. well-ordered), so is $\left(\overrightarrow{\bigoplus_{i\in\mathbb{N}}} \mathcal{E}_i, \preceq\right)$.*

Proof. We do the proof in the well-founded case; of course it proves the well-ordered case as well, but in this last case the reader may prefer to rewrite a proof which would look even more like a classical induction.

Let H be a hereditary subset of $\left(\overrightarrow{\bigoplus_{i\in\mathbb{N}}} \mathcal{E}_i, \preceq\right)$. Put $H_0 = H \cap \mathcal{E}_0$ (the $\mathcal{E}_i$ are viewed as included in their disjoint union). Then H_0 is a hereditary subset of $\mathcal{E}_0$: take $x \in \mathcal{E}_0$ such that all $x' \in \mathcal{E}_0$, $x' <_0 x$ is in H_0. Then all $y \in \overrightarrow{\bigoplus} \mathcal{E}_i$ such that $y < x$ is in $\mathcal{E}_0$, hence in $H_0 \subseteq H$; H being hereditary, we have $x \in H$, and $x \in H_0$. So H_0 is a hereditary subset; and we deduce that $H_0 = \mathcal{E}_0$.

Now put $H_1 = H \cap \mathcal{E}_1$. Let us show that H_1 is hereditary. Take $x \in \mathcal{E}_1$ such that all $x' <_1 x$ is in H_1. Take $y \in \overrightarrow{\bigoplus} \mathcal{E}_i$, $y < x$. Then either $y \in \mathcal{E}_0$ or $y \in \mathcal{E}_1$; in the first case, we have $\mathcal{E}_0 = H_0$, so $y \in H$ and in the second case $y <_1 x$ and $y \in H_1 \subseteq H$. H being hereditary, we have $x \in H$, and $x \in H_1$. So H_1 is a hereditary subset; and we deduce that $H_1 = \mathcal{E}_1$.

By induction, we obtain $\forall i$, $H \cap \mathcal{E}_i = \mathcal{E}_i$. So $H = \overrightarrow{\bigoplus} \mathcal{E}_i$. □

Corollary 2.3. *Let R be a coherent ring.*

- *If R is* ML*-Noetherian, then* $\left(\overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{R[X]_n}, \succeq\right)$ *is well-founded.*
- *If R is strongly Noetherian, then there exists a decreasing map Φ from* $\left(\overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{R[X]_n}, \preceq\right)$ *to a well-ordered set.*

Proof. The first point is now easy: if $(\mathcal{I}_R, \supseteq)$ is well-founded, then each of the $(\mathcal{I}_{R[X]_n}, \supseteq)$ is well-founded (Corollary 2.2), and we just apply the previous lemma.

Now the second point: assume we have decreasing maps

$$\begin{aligned}
&\phi_1 : \mathcal{I}_{R[X]_1} \longrightarrow \mathcal{E}_1\\
&\phi_2 : \mathcal{I}_{R[X]_2} \longrightarrow \mathcal{E}_2\\
&\vdots
\end{aligned}$$

to well-ordered sets $\mathcal{E}_0, \mathcal{E}_1, \ldots$. We define

$$\begin{aligned}
&\Phi : \overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{R[X]_n} \longrightarrow \overrightarrow{\bigoplus_{n\geq 1}} \mathcal{E}_n\\
&M \subseteq R[X]_n \mapsto \phi_n(M).
\end{aligned}$$

This is a decreasing map from $\left(\overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{R[X]_n}, \preceq\right)$ to the well-ordered set $\left(\overrightarrow{\bigoplus_{n\geq 1}} \mathcal{E}_n, \preceq\right)$. □

Let Θ be the following map

$$\begin{aligned}
&\Theta : \mathcal{I}_{R[X]} \longrightarrow \mathcal{I}_R \times \overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{R[X]_n}\\
&I \mapsto (\mathrm{LC}(I), I \cap R[X]_{n(I)}).
\end{aligned}$$

This is a decreasing map—the value set being ordered lexicographically. Indeed, of $I \subseteq J$ then $\text{LC}(I) \subseteq \text{LC}(J)$; and if $\text{LC}(I) = \text{LC}(J)$, then either $n(I) < n(J)$ or $n(I) = n(J)$ and in that case

$$I \cap R[X]_{n(I)} \subseteq J \cap R[X]_{n(J)}.$$

Moreover if $I \subseteq J$, $\text{LC}(I) = \text{LC}(J)$, $n(I) = n(J)$ and $I \cap R[X]_{n(I)} = J \cap R[X]_{n(J)}$, these last two submodules generating respectively I and J as an ideal, we have $I = J$.

Now we can state the following:

Theorem 2.1. *Let R be a coherent ring with detachable ideals. Then:*

- *If R is* ML*-Noetherian, so is $R[X]$.*
- *If R is strongly Noetherian, so is $R[X]$.*

In both cases, $R[X]$ is coherent and has detachable ideals.

Proof. For the first point, it is almost immediate: if the poset $(\mathcal{I}_R, \supseteq)$ is well-founded, so is $\left(\overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{R[X]_n}, \succeq\right)$, and $\left(\mathcal{I}_R \times \overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{R[X]_n}, \geq_{\text{lex}}\right)$. The map Θ together with the Lemma 2.3 gives the desired conclusion.

For the second point, since R is strongly Noetherian, we have a decreasing map $\phi : \mathcal{I}_R \longrightarrow \mathcal{E}$ where $\mathcal{E}$ is well-founded; and, from the previous corollary, a decreasing map

$$\Phi : \overleftarrow{\bigoplus_{n\geq 1}} \mathcal{I}_{R[X]_n} \longrightarrow \mathcal{F},$$

where $\mathcal{F}$ is well-founded. We can compose Θ with $\phi \times \Phi$ as follows:

$$\Psi : \mathcal{I}_{R[X]} \longrightarrow \mathcal{E} \cdot \mathcal{F}$$
$$I \mapsto (\phi(\text{LC}(I)), \Phi(I \cap R[X]_{n(I)}))$$

where $\mathcal{E} \cdot \mathcal{F}$ is $\mathcal{E} \times \mathcal{F}$ ordered lexicographically; Ψ is a decreasing map from $(\mathcal{I}_{R[X]}, \supseteq)$ to $(\mathcal{E} \cdot \mathcal{F}, \leq_{\text{lex}})$, a well-ordered set. $\square$

3. A particular case: $\mathbb{Z}[X_1, \ldots, X_d]$

In the proof of Proposition 2.3, we used implicitly the fact that if $\mathcal{E}_1$, $\mathcal{E}_2$ are posets, the identity is an increasing map from $\mathcal{E}_1 \times \mathcal{E}_2$ (ordered by the product order) to $\mathcal{E}_1 \cdot \mathcal{E}_2$ (ordered lexicographically). In some particular cases one can do better:

Lemma 3.1. *Let k, d be positive integers. Denote $(E, \leq) = (\mathbb{N}^k, \leq_{\text{lex}})$. There exists an increasing map from $(E^d, \leq_d)$ (ordered by the product order) to $(E, \leq)$.*

I thank Fred Richman who indicated to me the following nice proof.

Proof. It suffices to prove the result for $d = 2$; if there is an increasing map from $(E^d, \leq_d)$ to $(E, \leq)$, there is one from $(E^{d+1}, \leq_{d+1})$ to $(E^2, \leq_2)$, and we are done by induction.

Denote by $E \times F$ the direct product *ordered by the product order* and by $E \cdot F$ the direct product *ordered lexicographically*. Consider the class of ordered sets such that there is an increasing map from $E \times E$ to E. This class is closed under lexicographic products: the natural map

$$(E \cdot F) \times (G \cdot H) \longrightarrow (E \times G) \cdot (F \times H)$$

is increasing, so we get an increasing map from $(E \cdot \mathcal{F}) \times (E \cdot \mathcal{F})$ to $(E \times E) \cdot (F \times F)$, hence to $E \cdot F$. It suffices to construct an increasing map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. This is left to the reader. $\square$

Now we can give a variant of Corollary 2.2.

Lemma 3.2. *Let R be a coherent ring, with a decreasing map ϕ from $(\mathcal{I}_R, \subseteq)$ to $E = (\mathbb{N}^k, \leq)$. Then there exists a decreasing map from $(\mathcal{I}_{R^n}, \subseteq)$ (the submodules of R^n) to E.*

Lemma 3.3. *If for all i, $(\mathcal{E}_i, \leq_i) = (\mathbb{N}^k, \leq)$, then there is an order isomorphism between $(\mathbb{N}^{k+1}, \leq_{\text{lex}})$ and $\left(\overrightarrow{\bigoplus_{i \in \mathbb{N}}} \mathcal{E}_i, \preceq\right)$.*

Proof. Send $(a_0, a_1, \ldots, a_k) \in \mathbb{N}^{k+1}$ on $(a_1, \ldots, a_k) \in \mathcal{E}_{a_0} \subseteq \overrightarrow{\bigoplus_i} \mathcal{E}_I$. $\square$

Now it is easy to obtain the following corollary, as a variant of Theorem 2.1.

Corollary 3.1. *Let R be a coherent ring, and ϕ be a decreasing map from $(\mathcal{I}_R, \subseteq)$ to $(\mathbb{N}^k, \leq_{\text{lex}})$. Then there exists a decreasing map from $(\mathcal{I}_{R[X]}, \subseteq)$ to $(\mathbb{N}^{2k+1}, \leq_{\text{lex}})$.*

And now we have the following:

Proposition 3.1. *Let R be the polynomial ring $\mathbb{Z}[X_1, \ldots, X_d]$; there exists a decreasing map from $(\mathcal{I}_R, \subseteq)$ to $(\mathbb{N}^k, \leq_{\text{lex}})$, where $k = 2^{d+1} + 2^d - 1$.*

Proof. For $R = \mathbb{Z}$, we have a decreasing map from $\mathcal{I}_R$ to $\mathbb{N} \cup \{+\infty\}$, hence it is easy to construct a decreasing map from $\mathcal{I}_R$ to $(\mathbb{N}^2, \leq_{\text{lex}})$. We conclude by induction, using the previous corollary. $\square$

The value of k in the previous result is so high due to the inductive proof; as we already pointed out in the introduction, using Gröbner bases over a ring could improve this result dramatically.

4. Lasker–Noether rings

We discuss in this section the problem of deciding whether a finitely generated ideal I in a ring R is prime or not; then we get some results about the radical of a finitely generated ideal, or about its primary decomposition.

We provide an elementary solution. This question is not so often handled; some textbooks of computer algebra, such as Mishra (1993), provide a solution based on *characteristic sets*; Cox et al. (1992), among other computer algebra textbooks, refers to Mines et al. (1988) or even to Hermann (1926).

Let us recall that the *radical of an ideal* $I \subseteq R$ is defined by:

$$\sqrt{I} = \{x \in R : x^n \in I \text{ for some } n\}.$$

The solution in Mines et al. (1988) is to define a *Lasker–Noether ring* as a ring in which the radical of a finitely generated ideal I is (explicitly) the intersection of finitely many finitely generated prime ideals. An additional hypothesis allows one to define a *fully Lasker–Noether ring*, and to show a transfer theorem: if R is fully Lasker–Noether, so is $R[X]$.

We replace the hypothesis about radical ideals by the existence of a primality test; this seems more natural. The RS-*Noetherian* condition is not strong enough to show that this enables one to find the radical of an ideal as the intersection of prime ideals, but the strongly Noetherian condition will do the job.

4.1. Strong primality test and fully Lasker–Noether rings

Definition. A *strong primality test* for a ring R is an algorithm (or an oracle!) which decides, given a finite number of elements $a_1, \ldots, a_n \in R$, whether the ideal $I = a_1 \cdot R + \cdots + a_n \cdot R$ is prime or not, and if not, gives $a, b \in R$ such that $ab \in I$ and $a, b \notin I$.

The ability of performing a strong primality test in $F[X]$ is equivalent to the one of factorizing a polynomial $f(X) \in F[X]$. Following the terminology of Mines et al. (1988), a discrete field F is said to be *factorial* if we have a factorization algorithm in $F[X]$.

Definition. A *fully factorial field* F is a factorial field such that any finitely generated field extension of F is factorial.

Example 4.1. The prime fields $\mathbb{Q}$ and $\mathbb{F}_p$ are fully factorial.

For a complete discussion of fully factorial fields, see Mines et al. (1988). We are going to use again the terminology *fully Lasker–Noether ring*, but please note that our definition is different from the definition in Mines et al. (1988). It allows to give simpler proofs which are closer to classical proofs.

Definition. A ring is fully Lasker–Noether if

- It is a coherent, strongly Noetherian ring with detachable ideals.
- It has a strong primality test.
- If $\mathfrak{P}$ is a finitely generated prime ideal of R, the fraction field of $R/\mathfrak{P}$ is fully factorial.

Example 4.2. Any fully factorial field F is a fully Lasker–Noether ring, as well as the polynomial ring $F[X]$; the ring $\mathbb{Z}$ is fully Lasker–Noether.

We are going to prove the following transfer theorem.

Theorem 4.3. *If the ring R is fully Lasker–Noether, so is $R[X]$.*

Lemma 4.1. *Let R be a coherent strongly Noetherian integral domain with detachable ideals, and F its fraction field. Let $I = (f_1, \ldots, f_s)$ be a finitely generated ideal of $R[X]$,* *and I^e be $F \cdot I = f_1 \cdot F[X] + \cdots + f_s \cdot F[X]$, its extension to $F[X]$. One can compute a finite basis for the ideal $I^e \cap R[X]$.*

Proof. Let $g(x) \in R[X]$ be a single generator of I^e. Write $g(X) = a \cdot X^n + h(x)$ where $\deg h < n$.

A polynomial $f(X) \in R[X]$ is in $I^e \cap R[X]$ iff there exists $\alpha \in R$ such that $\alpha \cdot f \in g \cdot R[X]$. Suppose that this holds, and write $f = b \cdot X^m + h_1(X)$ with $\deg h_1 < m$; we claim that $a^{m-n+1} \cdot f \in g \cdot R[X]$.

First, R being an integral domain, it is clear that if $m < n$, then $f = 0$.

If $m = n$, then $a \cdot f - b \cdot g$ is in $I^e \cap R[X]$ and has degree $< n$, so it is zero, hence $a \cdot f \in I^e \cap R[X]$.

If $m > n$, then $f_1 = a \cdot f - b \cdot X^{m-n} \cdot g$ is in $I^e \cap R[X]$ and has degree $\leq m - 1$: by induction, we have $a^{m-n} f_1 \in g \cdot R[X]$, hence $a^{m-n+1} \cdot f \in I^e \cap R[X]$.

We have shown that

$$I^e \cap R[X] = \{f \in R[X] : a^m \cdot f \in g \cdot R[X] \text{ for some } m\}.$$

For $\alpha \in R$, we use the classical notation $(g : \alpha) = \{f \in R[X] : \alpha \cdot f \in g \cdot R[X]\}$. The ring $R[X]$ is coherent (Proposition 2.2), hence one can compute a finite basis for such an ideal $(g : \alpha)$.

Consider the increasing sequence of ideals

$$(g : a) \subseteq (g : a^2) \subseteq \cdots \subseteq (g : a^n) \subseteq \cdots.$$

Using Theorem 2.1, we see that $R[X]$ is Noetherian, so we find n such that $(g : a^n) = (g : a^{n+1})$. It is easy to verify that this implies $(g : a^n) = (g : a^{n+1}) = (g : a^{n+2}) = \cdots$, so that this ideal is precisely $I^e \cap R[X]$. $\square$

Lemma 4.2. *Let R be a coherent strongly Noetherian integral domain with detachable ideals, and F its fraction field. Let $I = (f_1, \ldots, f_s)$ be a finitely generated ideal of $R[X]$ such that $R \cap I = (0)$. If F is factorial, one can test the primality of I.*

Proof. We use the notation of the previous lemma. The polynomial $g(x) \in R[X]$ is a generator of I^e; if it is not irreducible in $F[X]$ it is easy to verify that I is not prime. Hence we assume that $g(X)$ is irreducible.

Compute a basis for $I^e \cap R[X]$. If $I \subsetneq I^e \cap R[X]$, then there is $g(X) \in R[X]$ and $\alpha \in R$ such that $g \notin I$ and $\alpha \cdot g \in I$; we have $I \cap R = (0)$ hence $\alpha \notin R$ and I is not prime.

Now if $I^e \cap R[X] = I$, the kernel of the canonical map $R[X] \longrightarrow F[X]/I^e$ is I, hence I is prime. $\square$

Proof of Theorem 4.3. The first point of the definition of the fully Lasker–Noether ring is verified, by Theorem 2.1.

Let $I = (f_1, \ldots, f_s)$ be a finitely generated ideal of $R[X]$. We can compute a basis of the finitely generated $\mathfrak{P} = I \cap R$, using Proposition 2.2. If $\mathfrak{P}$ is not prime, then I is not prime, and we are done.

If $\mathfrak{P}$ is prime let F be the fraction field of $R/\mathfrak{P}$; F is fully factorial.

Let $\overline{f}_1, \ldots, \overline{f}_s$ be the images of $f_1, \ldots, f_s$ under the canonical map from $R[X]$ to $R/\mathfrak{P}[X]$.

We are in the situation of Lemma 4.2: we can test whether $\overline{I} = (\overline{f}_1, \ldots, \overline{f}_s)$ is prime (as an ideal of $R/\mathfrak{P}[X]$) or not.

If it is prime the fraction field of $R[X]/I$ is isomorphic to $F[X]/\overline{I}^e$, that is, an algebraic extension of F; so it is fully factorial. □

Corollary 4.1.
- *If F is a fully factorial field, then $F[X_1, \ldots, X_n]$ is a fully Lasker–Noether ring.*
- *If the ring R is fully Lasker–Noether, so is $R[X_1, \ldots, X_n]$.*

So the class of fully Lasker–Noether rings is really wide: it is easy now to see that polynomial rings with coefficients in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{F}_q$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}(t)$, etc. are fully Lasker–Noether.

4.2. *Minimal primes over an ideal*

In a fully Lasker–Noether ring R, Theorem E from the introduction is true constructively, the termination of the algorithm given in the "computer algebra proof" being provable in strongly Noetherian rings: if $\phi : \mathcal{I}_R \longrightarrow E$ is a decreasing map to a well-ordered poset E, suppose that the algorithm ends for every ideal J such that $\phi(J) < \phi(I)$, then it ends for I, because if I is not prime the termination of the algorithm for I is equivalent to its termination for the two ideals $J_1 = I + aR \supset I$ and $J_2 = I + br \supset I$; we have $\phi(J_i) < \phi(I)$ for $i = 1, 2$, which concludes.

So given an ideal I there exists finitely many finitely generated prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_q$ containing I, such that if $\mathfrak{P}$ is a prime ideal containing I, there exists i such that $I \subseteq \mathfrak{P}_i \subseteq \mathfrak{P}$. We can keep only the minimal primes among the $\mathfrak{P}_i$, and of course remove the duplicates. So we get the following theorem:

Theorem 4.4. *Let R be a fully Lasker–Noether ring. Let I be a finitely generated ideal of R; there exists finitely many finitely generated minimal prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ containing I.*

This existential statement is to be read in the constructive sense.

Now the following is a classical result:

Proposition 4.1. *The radical of I is the intersection of the minimal primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ containing I.*

Proof. We postpone the proof to the next subsection. □

4.3. *Some ideas from dynamical algebra*

We are not going to do *dynamical algebra* as in Coste et al. (2001), but we will use some ideas of this paper.

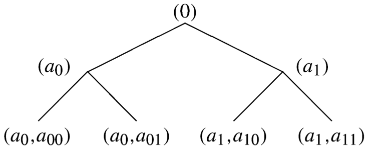
In a fully Lasker–Noether ring, there are finitely many minimal prime ideals—just apply Theorem 4.4 to the ideal $I = (0)$. The intersection of these ideals is the *nilradical* of R, denoted by $N(R)$.

We are going to show that

$$N(R) = \{x : x^n = 0 \text{ for some } n\}.$$

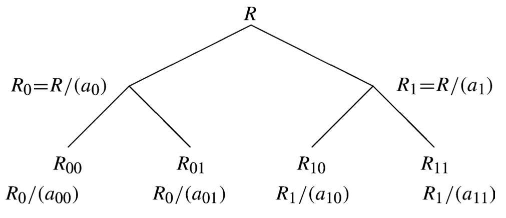
Applying this result to R/I, we obtain Proposition 4.1 (we leave it to the reader to verify that if R is fully Lasker–Noether, so is R/I).

The only thing to prove is that if x is in each of the ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_q$, it is nilpotent. The $\mathfrak{P}_i$'s are obtained at the leaves of a tree constructed as in the Introduction:



with $a_0 \cdot a_1 = 0$, $a_{00} \cdot a_{01} \in (a_0)$, $a_{10} \cdot a_{11} \in (a_1)$, and so on.

We change the labels of the nodes of the tree in rings, in the following way:



At the leaves of the tree, we have rings in which the image of $x \in R$ under the canonical projection is 0.

Lemma 4.3. *Let R be a discrete ring, and $a, b \in R$ be non-zero elements such that $ab = 0$. Put $R_0 = R/(a)$ and $R_1 = R/(b)$, and let ϕ_0, ϕ_1 be the associated canonical projections.*

If $\phi_0(x)$ and $\phi_1(x)$ are nilpotent respectively in R_0 and R_1, so is x in R.

Proof. We have $\phi_0(x)^n = 0$ and $\phi_1(x)^m = 0$, that is, in R, $x^n = \lambda \cdot a$ and $x^m = \lambda \cdot b$, with $\lambda, \mu \in R$. We get $x^{n+m} = \lambda\mu \cdot ab = 0$. $\square$

This terminates our proof: just propagate the equalities found in the leaves of the tree back to the root—the operation to be performed at each node is given by the previous lemma.

4.4. *The primary decomposition*

We outline roughly how a primary decomposition can be obtained in a fully Lasker–Noether ring R. An elementary classical exposition of this topic can be found in Sharp (2000, Chapter 4).

Definition.
- An ideal $\mathfrak{Q} \subseteq R$ is a *primary ideal* if $ab \in \mathfrak{Q}$ implies $b \in \mathfrak{Q}$ or $a^n \in \mathfrak{Q}$ for some $n \in \mathbb{N}$.
- A *primary decomposition* of an ideal I is a finite family of finitely generated primary ideals $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$, such that $I = \mathfrak{Q}_1 \cap \cdots \cap \mathfrak{Q}_r$.

One can prove that in a ring satisfying the fully Lasker–Noether, any finitely generated ideal has a primary decomposition.

Step 1. We give a primarity test for finitely generated ideals of R: given $I = (a_1, \ldots, a_n)$, decide whether I is primary or not, and if not, give a, b such that $ab \in I$, $b \notin I$ and $a^n \notin I$ for all $n \in \mathbb{N}$.

We know that an ideal is primary iff there is only one minimal prime containing it, cf. Sharp (2000). So we use Theorem 4.4 to find the minimal primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ containing I. If $r > 1$ take for each $i = 1, \ldots, r$ some $x_i \in \mathfrak{P}_i$ such that $x_i \notin \sqrt{I} = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_r$. The product $x_1 \cdots x_r$ is in $\sqrt{I}$. Then there is some i such that $x_1 \cdots x_{i-1} \notin \sqrt{I}$ and $x_1 \cdots x_i \in \sqrt{I}$: put $a_0 = x_1 \cdots x_{i-1}$ and $b_0 = x_i$. Now $a_0 \notin \sqrt{I}$, $b_0 \notin \sqrt{I}$, and $a_0 \cdot b_0 \in \sqrt{I}$; take some $k \in \mathbb{N}$ such that $(a_0 \cdot b_0)^k \in I$, and let $a = a_0^k$ and $b = b_0^k$. The ideal $\sqrt{I}$ being radical, $a_0, b_0 \notin \sqrt{I}$ implies $a, b \notin \sqrt{I}$, and for all $n \in \mathbb{N}\, a^n \notin I$.

Step 2. Find an n such that $(I : a^n) = (I : a^{n+1})$. *(Note that* $(I : x) = \{y \in R : xy \in I\}$*.)*

In a coherent ring, one can compute bases for the ideals $(I : a^n)$, cf. Mines et al. (1988). The constructive ascending chain condition **ACC** on the ideals of R suffices to prove that such an n exists. We can find it by successive tries.

Step 3. We show that $I = (I + a^n \cdot R) \cap (I + b \cdot R)$.

This comes from the proof of Proposition 4.34, in Sharp (2000). First clearly $I \subseteq (I + a^n \cdot R) \cap (I + b \cdot R)$.

Now if $r \in (I + a^n \cdot R) \cap (I + b \cdot R)$, then $r = g + c \cdot a^n = h + d \cdot b$ for some $g, h \in I$ and $c, d \in R$. Hence $c \cdot a^{n+1} = h \cdot a + d \cdot a \cdot b - g \cdot a \in I$, and $c \in (I : a^{n+1}) = (I : a^n)$. Then $c \cdot a^n \in I$ and r is in I, which achieves the proof.

Step 4. It is now easy to conclude by a “growing tree algorithm”, in the spirit of Theorem E. At each leaf of the growing tree, if the ideal is not primary, Steps 1 to 3 show how to obtain two new leaves. The proof of termination is exactly as the proof given for Theorem E in Section 4.2.

5. As a conclusion, some remarks

Grete Hermann explicitly asked for an algorithmic proof to provide *bounds* for the termination of an algorithm; she refused any abstract proof of termination. For example she would have refused the classical proof of termination of Buchberger’s Algorithm.

Our proof, as stated here, does not give explicit bounds; but these proofs are constructive proofs, and one can obtain bounds by analyzing the proof. Unfortunately, these bounds are not primitive recursive in the parameters d and n (where d is the number of variables, and n the maximum degree of polynomial in a basis $f_1, \ldots, f_s$ of I), as shown in Perdry (2001); so the existence of these bounds has no practical interest.

Our definition of Noetherian has a very concrete statement and is nevertheless strong enough to prove constructively the termination of algorithms involving “trees of ideals”; the efficiency of such algorithms (at least for providing clear and intuitive constructive proofs) has been illustrated in the last section.

An interesting problem would be to find explicitly the smallest well-founded set which can be associated to a Noetherian ring, which is a measure of “complexity” of the posets of ideals of this ring.

Acknowledgements

I thank Fred Richman for the proof of Lemma 3.1, and Henri Lombardi for many stimulating discussions. I am grateful to Claude Quitté for finding a gap in a proof in an early version. I thank the referees for many useful questions and suggestions; I feel greatly indebted to David Cox for his careful reading and his detailed comments.

References

Adams, W.W., Loustaunau, P., 1994. An Introduction to Gröbner Bases. American Mathematical Society, Providence, RI.

Beeson, M.J., 1985. Foundations of Constructive Mathematics. Metamathematical Studies, Springer-Verlag, Berlin.

Bishop, E., 1967. Foundations of Constructive Analysis. McGraw-Hill Book Co.

Buchberger, B., 1965. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal, Innsbruck Universität, Dissertation.

Buchberger, B., 1970. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. Aequationes Math. 4, 374–383.

Coste, M., Lombardi, H., Roy, M.-F., 2001. Dynamical method in algebra: effective Nullstellensätze. Ann. Pure Appl. Logic 111 (3), 203–256.

Cox, D.A., Little, J.B., O'Shea, D., 1992. Ideals, Varieties, and Algorithms. Springer-Verlag, New York.

Gordan, P., 1899. Neuer Beweis des Hilbertsche Satzes über homogene Funktionen. Nachr. Gesell. der Wissen. zu Göttingen 2, 240–242. Available from http://gdz.sub.uni-goettingen.de/.

Hermann, G., 1926. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann 95, 736–788.

Hermann, G., 1998. The question of finitely many steps in polynomial ideal theory. SIGSAM Bulletin 32 (3), 8–27.

Hilbert, D., 1890. Ueber die theorie der algebraischen formen. Math. Ann. 36, 473–534.

Jacobsson, C., Löfwall, C., 1991. Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem. J. Symbolic Comput. 12, 337–371.

Lombardi, H., Perdry, H., 1998. The Buchberger algorithm as a tool for ideal theory of polynomials rings in constructive mathematics. In: Proc. of the Conference 33 Years of Gröbner Bases. In: Gröbner Bases and Applications. London Mathematical Society Lecture Notes Series, vol. 251. Cambridge University Press.

Malliavin, M.-P., 1985. Algèbre Commutative. Masson, Paris.

Mines, R., Richman, F., Ruitenburg, W., 1988. A Course in Constructive Algebra. Springer-Verlag, New York.

Mishra, B., 1993. Algorithmic Algebra. Springer-Verlag, New York.

Perdry, H., 2001. Aspects constructifs de la théorie des corps valués, Université de Franche-Comté, Thèse précédée d'un chapitre sur la noethérianité constructive.

Richman, F., 1974. Constructive aspects of Noetherian rings. Proc. Amer. Mat. Soc. 44, 436–441.

Seidenberg, A., 1974. What is Noetherian? Rend. Sem. Mat. Fis. Milano 44, 55–61.

Sharp, R.Y., 2000. Steps in Commutative Algebra, second ed. Cambridge University Press, Cambridge.